FRVT MORPH: Face Morph Detection Evaluation

Mei Ngan, *Patrick Grother, and Kayee Hanaoka*
National Institute of Standards & Technology

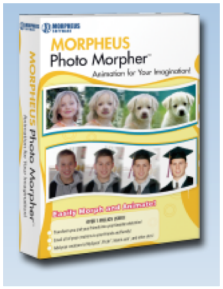
International Face Performance Conference
November 28, 2018
NIST, Gaithersburg, MD

INFORMATION TECHNOLOGY LABORATORY

Face Morphing

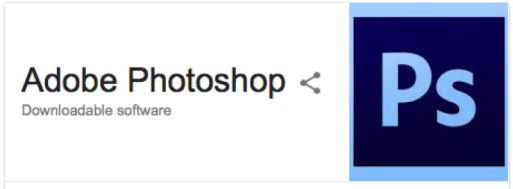
Face Morphing Software

Desktop Apps



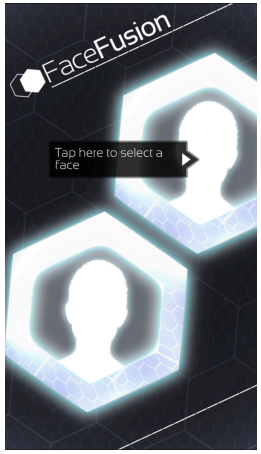
Source: http://www.morpheussoftware.net

Source: http://www.fantamorph.com



Source: https://www.adobe.com/products/photoshop.html

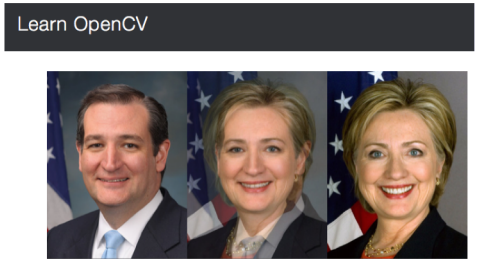
Mobile Apps



Source: https://en.softonic.com/solutions/apps/facefusion-lite

Source: http://www.piviandco.com/apps/mixbooth

Automated methods



Source: https://www.learnopencv.com/face-morph-using-opencv-cpp-python

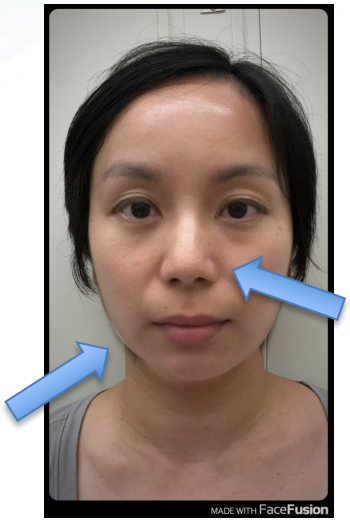
Websites

Source: http://www.morphthing.com

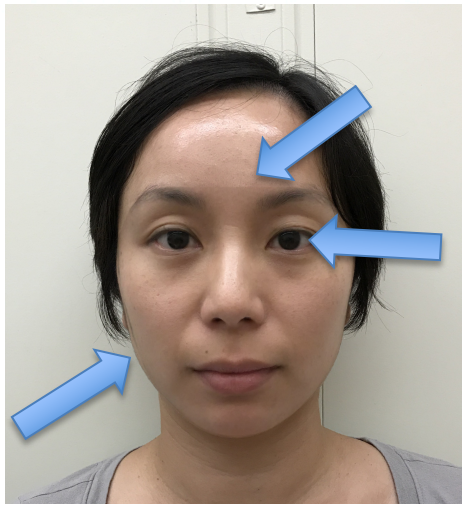
Morph Examples


+

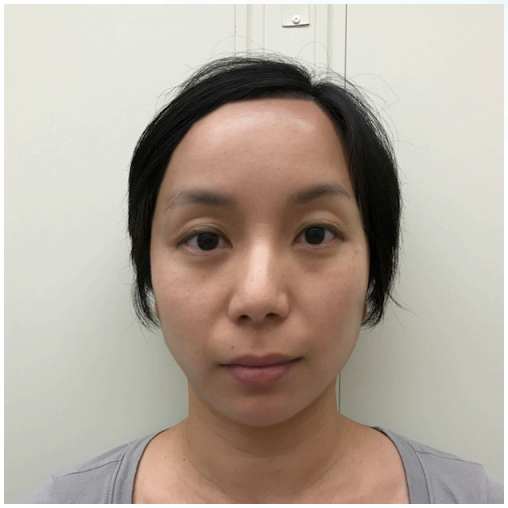

www.MorphThing.com



FaceFusion Mobile App



Automated Method[1-3]



FantaMorph + Photoshop

[1] M. Ferrara, A. Franco, and D. Maltoni, "Face Demorphing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 1008-1017, April 2018.
[2] M. Ferrara, A. Franco, and D. Maltoni, "The Magic Passport," in IEEE International Joint Conference on Biometrics (IJCB), Clearwater, Florida, USA, 2014, pp. 1-7.
[3] M. Ferrara, A. Franco, and D. Maltoni, "On the Effects of Image Alterations on Face Recognition Accuracy," in Face Recognition Across the Electromagnetic Spectrum. Switzerland: Springer International Publishing, 2016, pp. 195-222.

Existence Proof (c. 2014)

University of Bologna

- One morphing algorithm
- Two FR algorithms vulnerable
  - Luxand
  - Neurotechnology
  - Threshold set for FMR = 0.001
- All frauds successful:
  - Male-Male (5 pairs)
  - Female-Female (5 pairs)
  - Male-Female (1 pair)
  - Male-Male-Male (1 triple)
  - Close age pairings

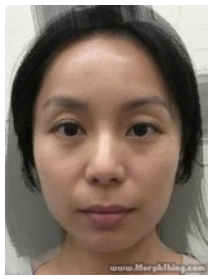
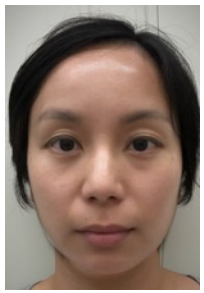
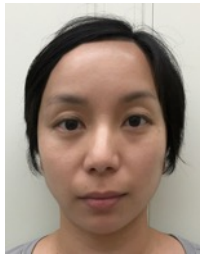
Ferrara, Franco, and Maltoni, ***The Magic Passport***, IEEE International Joint Conference on Biometrics, October 2014, pp. 1-7

NIST

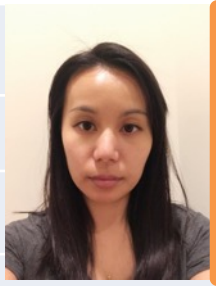
- Two morphing algorithms
- Twelve FR algorithms vulnerable
- Most frauds successful:
  - Male-Male (5 subjects)
  - No algorithm immune

Conclusion: Existence proof - morphed images can match two people strongly




1.983	1.842
3958	3497
86.75	84.44
1.883	2.000
3727	3846
86.41	88.46
1.997	1.839
3814	3609
86.42	84.56
1.965	1.836
3761	3542
85.65	82.58

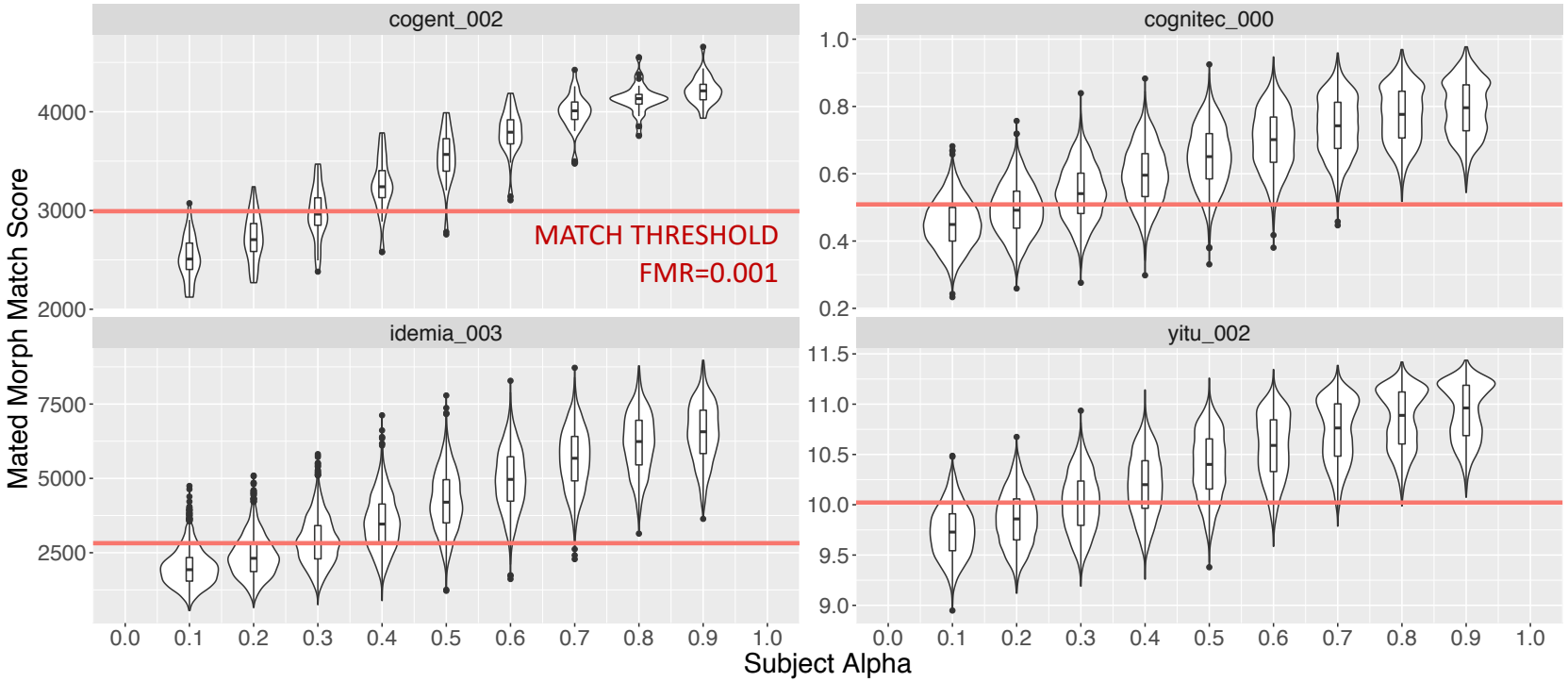
NTechLab		1.428
Gemalto		2634
Megvii/Face++		61.65

Scores above matching thresholds: **Both** subjects authenticate against all morphs at FMR = 0.001 AND FMR = 0.00001!

Subjects do NOT authenticate at weak FMR = 0.001, because they're naturally different people

Face matching algorithm (2018)	Threshold for FMR=0.001	Threshold for FMR=0.00001
NTechLab	1.451	1.542
Gemalto	2847	3039
Megvii/Face++	68.65	79.09

Face recognition algorithms (October 2018) are still vulnerable



- 2-person morphs
  - subject alpha ranged from 0.1 -> 0.9 per pair
  - morphed within race and gender label groups
  - 24,228 comparisons of morphs with constituents
- > 30 million non-morph comparisons to generate FMR threshold

NIST FRVT MORPH

Automated Face Morph Detection Evaluation

- Single-image morph detection
- Single-image scanned morph detection
- Two-image differential morph detection
- 1:1 morph acceptance (FR resistance against morphing)

Currently Seeking…

- Developers of morph detection technology
- Collaboration partners with suitable morph data or software that can be shared with NIST

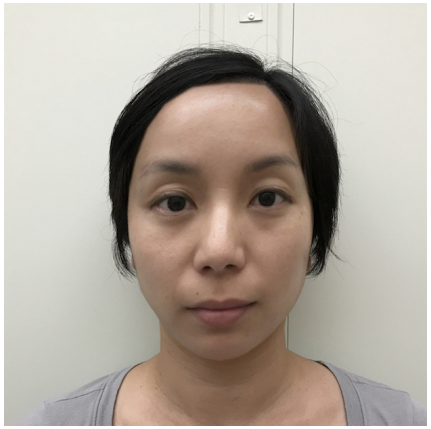
BREAKING NEWS

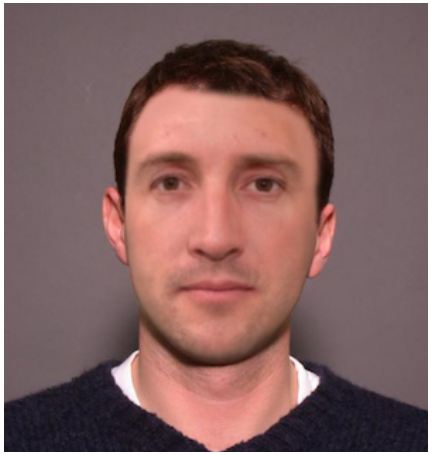
Face Recognition Vendor Test (FRVT) MORPH Evaluation

Now Accepting algorithm submissions! Google: FRVT MORPH

LIVE NIST

Single Image Morph Detection: *Morphed image or not?*





Use Case: Attack on enrollment

- Untrusted capture
- Upload to server

Protocol: Given **single image** X in isolation, produce

1) Morph decision
2) "morphiness" score

Morphiness = F(X)

Evaluation: ISO/IEC 30107-3 metrics

- Attack Presentation Classification Error Rate (APCER): proportion of morph attack samples incorrectly classified as bona fide presentation (missed detection rate over morphed images)
- Bona Fide Presentation Classification Error Rate (BPCER): proportion of bona fide samples incorrectly classified as morphed samples (false detection rate over un-morphed images)
- Others TBD

Two-Image Differential Morph Detection: *Morph detection given live image?*

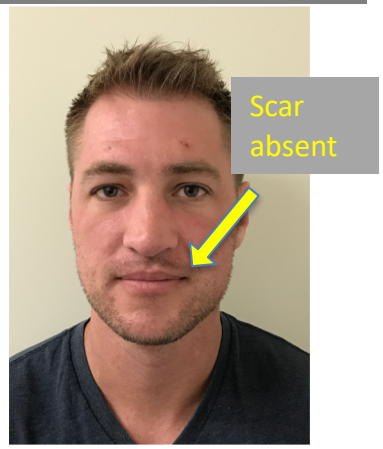
Use Case: Attack during verification (e.g., at eGate)

- Prior morph enrolled e.g. on identity document

C = A+B. Morphed image is contained in a passport

A. Images of this image not available during authentication

B2: This image represents a live capture during an eGate border crossing, say.



Protocol: Given image X and suspected morph Y produce

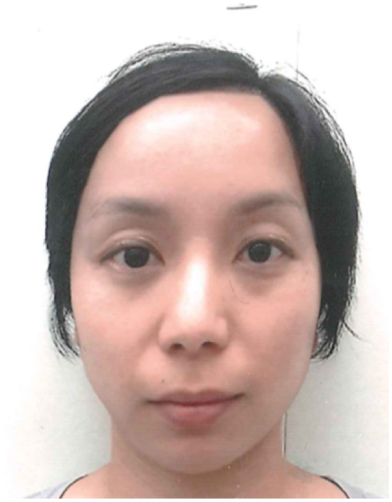
1) Morph decision
2) "morphiness" score

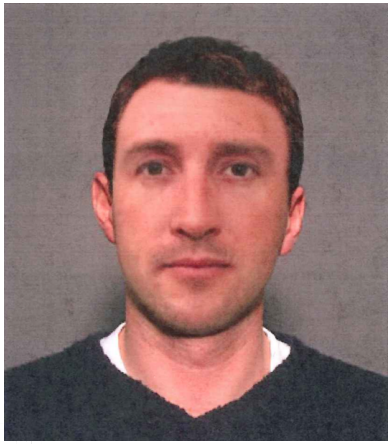
Evaluation: ISO/IEC 30107-3 metrics

- BPCER
- APCER
- Others TBD

Goal: Determine that image C is morphed by finding features in it that are not present in image B2. For example, the scar should be present but is not.

Single Image Scanned Morph Detection:
Morphed image or not?





Use Case: Attack on enrollment

- Untrusted capture
- Upload to server

Protocol: Given **single printed + scanned image** X in isolation, produce

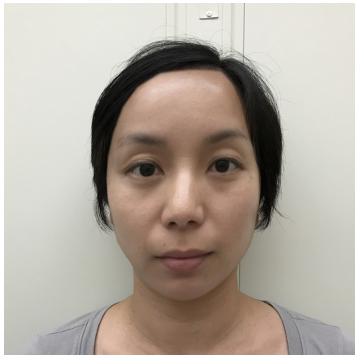
1) Morph decision
2) "morphiness" score

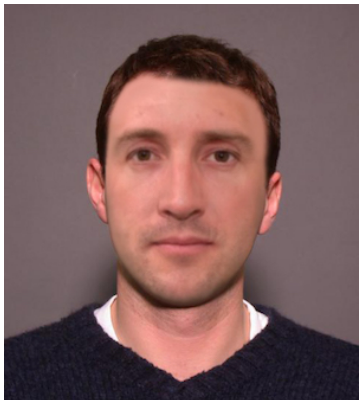
Morphiness = F(X)

Evaluation: ISO/IEC 30107-3 metrics

- BPCER
- APCER
- Others TBD

1:1 Morph Acceptance: *Do subjects verify successfully against morphed image?*





Use Case: Test FR algorithm resistance against morphing

Protocol: Given image X and image Y, produce verification similarity score

Evaluation: ISO/IEC 30107-3 metrics

- Mated Morph Presentation Match Rate (MMPMR)
- True Accept Rate
- False Accept Rate
- Others TBD

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Initial Test Data

- Tiered Approach
  - Morphs created with easily accessible morphing software (e.g. websites, mobile apps, etc.)
  - Morphs created with automated morphing algorithms
  - High quality morphs created manually with commercial tools (e.g. Photoshop, etc.)
- Factors
  - Alpha (subject % in morph)
  - Printing and Scanning
  - Compression Ratio/Resolution
  - Others
- New morph techniques/data TBD… open-ended

How to participate

[https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-morph]

Draft Evaluation Plan and API	*Developers send comments to NIST* [frvt@nist.gov]
Final Evaluation Plan and API	*Developers start implementing to final API* [https://www.nist.gov/sites/default/files/documents/2018/09/07/frvt_morph_api_v1.1.pdf]
Participation Agreement	*Developers send signed participation agreement to NIST* [https://www.nist.gov/sites/default/files/documents/2018/01/12/frvt_morph_participation_agreement.pdf]
Validation Package/ API Software	*NIST publishes validation package (with null or reference implementation)* *Developers must run their software against validation package* [https://github.com/usnistgov/frvt/tree/master/morph]
Algorithm submission	*Developers submit their validation results + algorithm to NIST* *NIST executes algorithm against datasets*
Ongoing Reporting	*NIST reports results back to participants and community* [https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-morph]

Thank you!

Mei Ngan
[mei@nist.gov]

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce